Malware Protection Guide: Defensive Layer 3

# Malware Protection Guide: Defensive Layer 3

**Parent topic:** [Malware Protection Guide - Overview](malware-protection-guide-introduction.html)

## Introduction

This guide explains the types of controls that need to be implemented to form the third of three layers of defence. Layer 3 helps reduce the impact of malware infection in two ways:

* reducing the ability for malware to move across networks
* ensuring that data is backed up

This guide is a sub-page to the [Malware Protection Guide](malware-protection-guide-introduction.html).

### Who is this for?

This Malware Protection information is mainly intended for in-house Ministry of Justice (MoJ) Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.

Other MoJ bodies, agencies, contractors, or IT suppliers and partners who in any way design, develop or supply services (including processing, transmitting and storing data) for, or on behalf of the MoJ, will also find this information helpful.

## Defensive Layer 3: Resilience and Rapid Response

Even with the controls created by defensive layers 1 and 2, it is still possible that malware might reside and execute on the MoJ networks. The following controls can help to build resilience, ensure a rapid response to infection, and reduce the impact of a successful malware intrusion:

|  |
| --- |
| Do |
| ✔ Ensure that applications, services or systems are segregated from the rest of the network as soon as they are no longer supported by the vendor or by MoJ teams. The NCSC provides guidance on how to implement [segregation of unsupported platforms](https://www.ncsc.gov.uk/guidance/obsolete-platforms-security-guidance). |
| ✔ If you are designing a system, ensure that it can make regular, reliable backups of data. This is to limit the amount of data corrupted, encrypted or lost if an application, service or system is infected with malware. |
| ✔ Ensure that backups meet all the criteria in [Note 1](#X533d333d505a9d17515c29ad729b61f17902b08). The [NCSC](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world) provides further guidance on data backups stored in public cloud environments. |
| ✔ Make sure that user permissions are regularly reviewed. Access to systems or drives no longer required by users must be removed. This is especially important for administrator accounts. See the [Access Control Guide](access-control-guide.html) for further information. |
| ✔ When managing a system, ensure that backups are conducted in line with the system requirements outlined in the IRAR. |
| ✔ Prioritise patches and updates of devices that perform security-related functions on the MoJ network. This includes firewalls and any device on the network boundary. See the [Vulnerability Scanning and Patch Management Guide](vulnerability-scanning.html) for further details. |
| ✔ Conduct regular audits of the software and data held on systems which support critical business processes. Check if they have been modified by malicious code. |
| ✔ Isolate critical MoJ environments from the wider network as much as possible. This is to avoid significant business impact that might occur if the wider network is compromised by malware. |

|  |
| --- |
| Don't |
| ✖ Use the same browser to conduct administrative activities that you use for general user activities. An example admin activity is changing access privileges. An example general user activity is searching the internet. Separating browsers for different activities can reduce the impact of malware attacks. |
| ✖ Delay implementing security patches on infrastructure. See the [Vulnerability Scanning and Patch Management Guide](vulnerability-scanning.html) for further information. |
| ✖ Delay if you suspect a malware incident has occurred. Make sure you contact the [Technology Service Desk](#contact-details) immediately. |

### Note 1

Important: Ensure that backups:

* can be recovered. Some cloud providers allow data restoration from a point in time. This can be helpful if malware affects the cloud backup.
* have an offline copy held in a separate location to the primary data storage. These are called cold backups and should be unaffected if an incident affects the primary environment
* are updated and tested regularly. The regularity of backups should be outlined in the system's Information Risk Assessment Report (IRAR), which is normally completed by Security Architects and Risk Assessors, in conversation with the system architects, designers and developers. The IRAR document must also be agreed with the Business Continuity Team. For more information regarding IRARs, and how to create and maintain them, contact the [Cyber Assistance Team](#contact-details).

## Preventing and Detecting Lateral Movement

One of the most important ways of limiting the spread of malware on the network is to reduce lateral movement. This is where a malware problem 'jumps across' from system to system. The main ways to prevent lateral movement are covered in the tables below.

|  |
| --- |
| Do |
| ✔ Make sure user credentials are protected. Do this using strong passwords which are stored securely. See the [Password Manager Guide](password-managers.html) for further information. |
| ✔ Ensure that effective access controls are designed and implemented in MoJ systems. Use [Multi-Factor Authentication (MFA)](multi-factor-authentication-mfa-guide.html) wherever possible. See the [Access Control Guide](access-control-guide.html) for further information. |
| ✔ Make sure you protect highly privileged accounts, by applying the principle of least privilege. See the [Access Control Guide](access-control-guide.html) for further information. |
| ✔ Ensure that any system or application running on the MoJ's networks can collect and share system logs with the Operational Security Team's (OST) central monitoring function. This allows the MoJ to detect lateral movement by malware. |
| ✔ Use tools for monitoring account activity, and look for indicators of account compromise. Examples include using [Conditional Access](https://en.wikipedia.org/wiki/Conditional_access) to manage access to the network, and detecting impossible geographical travel scenarios. Configure the tools to respond promptly by raising security alerts and so helping prevent a breach. |
| ✔ In the exceptional circumstances where Bring your Own Device (BYOD) is permitted to access MoJ information, make sure your device runs anti-malware software and follows the requirements in the [BYOD guidance](personal-devices.html). Also ensure that users can only access MoJ emails through approved applications. |
| ✔ If you are designing or modifying networks, ensure there is network segregation for systems and data that do not need to interact. This segregation can be achieved using physical or logical separation. Access between network domains is allowed, but must be controlled at the perimeter using a gateway such as a firewall. |

|  |
| --- |
| Don't |
| ✖ Access emails through third party applications which have not been approved by the MoJ. |
| ✖ Allow access to information on devices, by default. Restrict access on devices to need to know. |
| ✖ Use your administrator account for any non-administrative functions. Access should only be elevated for the specific tasks required, and only while the task is performed. See the Privileged User guidance for further details. |

The NCSC provides helpful guidance on preventing [lateral movement](https://www.ncsc.gov.uk/guidance/preventing-lateral-movement) across networks.

## Contact details

* Contact the Cyber Assistance Team for advice on protecting against malware - [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk)
* Contact the Technology Service Desk to report suspected malware:Telephone: 0800 917 5148.
* Contact the Operational Security Team (OST) - [Operationalsecurityteam@justice.gov.uk](mailto:Operationalsecurityteam@justice.gov.uk)